

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-330871

(43)Date of publication of application : 30.11.2000

(51)Int.Cl. G06F 12/14
G11B 20/10
// G09C 1/00

(21)Application number : 11-141269

(71)Applicant : VICTOR CO OF JAPAN LTD

(22)Date of filing : 21.05.1999

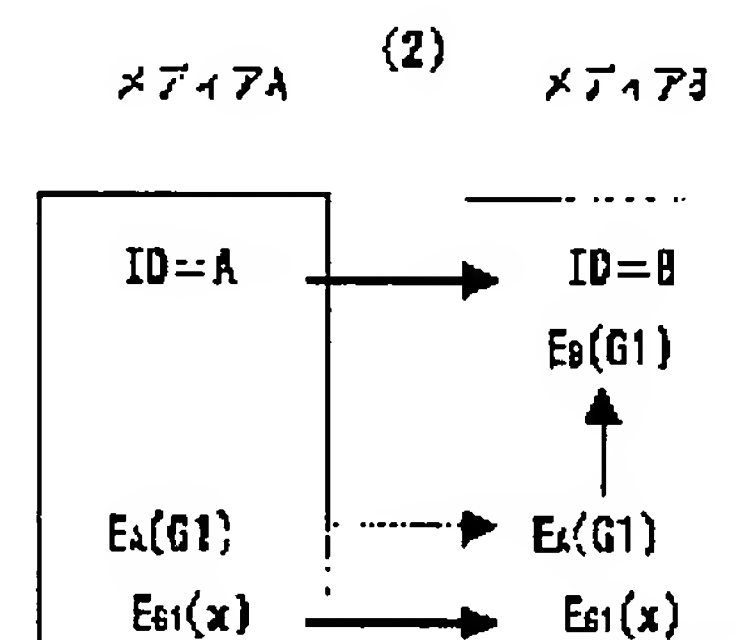
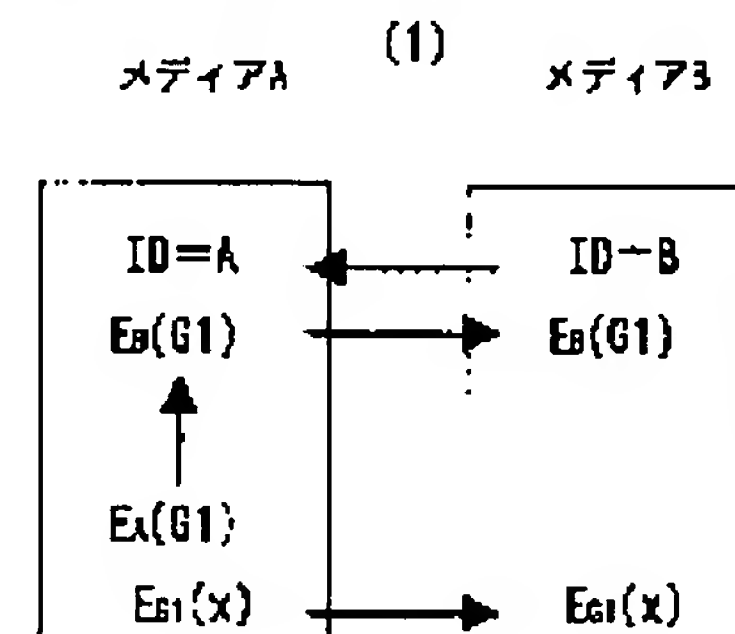
(72)Inventor : SUGAWARA TAKAYUKI

(54) METHOD AND DEVICE FOR RECORDING CONTENTS INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To record contents data by plural users while preventing the unauthorized copy of the contents data.

SOLUTION: In the case of recording ciphered contents information EG1 (x) from a medium A to a medium B, the medium A side reads out the ID=B of the medium B for receiving a copy, deciphers 1st ciphered key information EA (G1) previously ciphered by the ID=A of the medium A, ciphers the deciphered information again by the ID=B of the medium B, and transfers 2nd ciphered key information EB (G1) to the medium B.



LEGAL STATUS

[Date of request for examination]

28.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

THIS PAGE BLANK (USPTO)

[Date of final disposal for application]

[Patent number] 3682840

[Date of registration] 03.06.2005

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2000-330871

(P2000-330871A)

(43) 公開日 平成12年11月30日(2000.11.30)

(51) Int. Cl. 7	識別記号	F I	テ-マ-コ-ト(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14 3 2 0 B	5B017
G 1 1 B 20/10		G 1 1 B 20/10 H	5D044
// G 0 9 C 1/00	6 6 0	G 0 9 C 1/00 6 6 0 F	5J104
			9A001

審査請求 未請求 請求項の数 16 O L

(全 15 頁)

(21) 出願番号 特願平11-141269

(22) 出願日 平成11年5月21日(1999.5.21)

(71) 出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町3丁目12番地

(72) 発明者 菅原 隆幸

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

Fターム(参考) 5B017 AA06 BA05 BA07 BB03 BB10
CA16
5D044 AB05 AB07 DE48 GK17 HL06
HL11
5J104 AA16 EA26 JA03 NA02 NA05
NA36 PA10 PA14
9A001 EE03 JZ71 LL03

(54) 【発明の名称】 コンテンツ情報記録方法及びコンテンツ情報記録装置

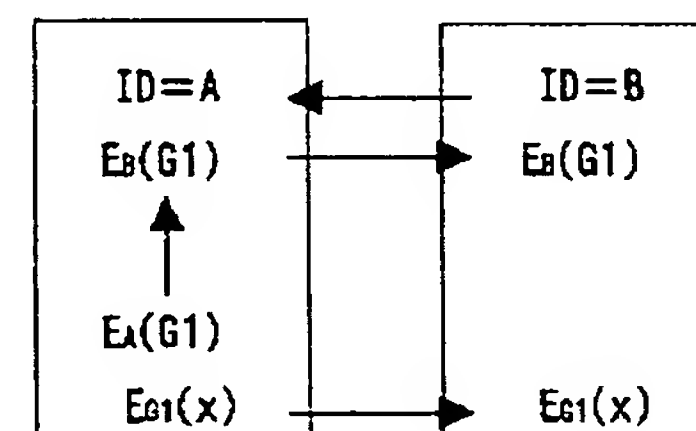
(57) 【要約】

【課題】 不正なコピーを防止しつつ、コンテンツデータのユーザー間での記録を可能とする。

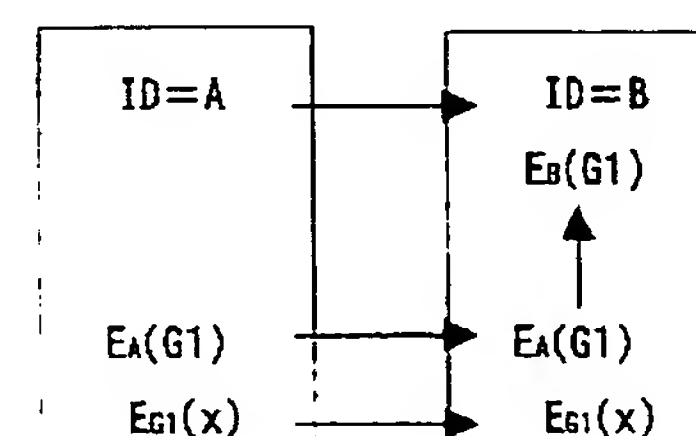
【解決手段】 暗号化コンテンツ情報EG1(X)をメディアAからメディアBに記録したときに、メディアA側でコピー先メディアのID=Bを読み取り、先にメディアA側でID=Aで暗号化された第1の暗号化鍵情報EA(G1)を復号し、コピー先のID=Bで再暗号化して第2の暗号化鍵情報EB(G1)にしてメディアBに転送する。

図 4

メディアA (1) メディアB



メディアA (2) メディアB



【特許請求の範囲】

【請求項 1】第 1 のメディアの ID に関する情報を ID 鍵としてコンテンツ情報を暗号化した第 1 の暗号化コンテンツ情報が記録された前記第 1 のメディアから、前記コンテンツ情報を第 2 のメディアに記録する際に、前記第 1 のメディア側から前記第 1 の暗号化コンテンツ情報を前記第 2 のメディア側に出し、前記第 2 のメディア側で、前記第 1 のメディア側から得た前記第 1 のメディアの ID に関する情報により一旦前記第 1 の暗号化コンテンツ情報の暗号を解き、前記第 2 のメディアの ID に関する情報を ID 鍵として前記コンテンツ情報を再暗号化した第 2 の暗号化コンテンツ情報を前記第 2 のメディアに記録することを特徴とするコンテンツ情報記録方法。

【請求項 2】第 1 のメディアの ID に関する情報を ID 鍵としてコンテンツ情報を暗号化した第 1 の暗号化コンテンツ情報が記録された前記第 1 のメディアから、前記コンテンツ情報を第 2 のメディアに記録する際に、前記第 1 のメディア側で、一旦前記第 1 の暗号化コンテンツ情報の暗号を解き、前記第 2 のメディア側から得た前記第 2 のメディアの ID に関する情報を ID 鍵として前記コンテンツ情報を再暗号化して第 2 の暗号化コンテンツ情報を得、その第 2 の暗号化コンテンツ情報を前記第 2 のメディア側に出し、前記第 2 のメディア側で、前記第 2 の暗号化コンテンツ情報を前記第 2 のメディアに記録することを特徴とするコンテンツ情報記録方法。

【請求項 3】第 1 のメディアの ID に関する情報を ID 鍵としてコンテンツ情報を暗号化した第 1 の暗号化コンテンツ情報が記録された前記第 1 のメディアから、前記コンテンツ情報を第 2 のメディアに記録する際に、下記方法 [a] と方法 [b] とを選択することを特徴とするコンテンツ情報記録方法。

方法 [a]

前記第 1 のメディア側から前記第 1 の暗号化コンテンツ情報を前記第 2 のメディア側に出し、前記第 2 のメディア側で、前記第 1 のメディア側から得た前記第 1 のメディアの ID に関する情報により一旦前記第 1 の暗号化コンテンツ情報の暗号を解き、前記第 2 のメディアの ID に関する情報を ID 鍵として前記コンテンツ情報を再暗号化した第 2 の暗号化コンテンツ情報を前記第 2 のメディアに記録する。

方法 [b]

前記第 1 のメディア側で、一旦前記第 1 の暗号化コンテンツ情報の暗号を解き、前記第 2 のメディア側から得た前記第 2 のメディアの ID に関する情報を ID 鍵として前記コンテンツ情報を再暗号化して第 2 の暗号化コンテンツ情報を得、その第 2 の暗号化コンテンツ情報を前記第 2 のメディア側に出し、前記第 2 のメディア側で、前記第 2 の暗号化コンテンツ

情報を前記第 2 のメディアに記録する。

【請求項 4】請求項 1～3 のいずれか一つに記載のコンテンツ情報記録方法において、

前記第 1 の暗号化コンテンツ情報の ID 鍵は、前記第 1 のメディアの ID をそのまま用いた共通鍵または前記第 1 のメディアの ID を所定の関数により変換した情報を用いた共通鍵であり、

前記第 2 の暗号化コンテンツ情報の ID 鍵は、前記第 2 のメディアの ID をそのまま用いた共通鍵または前記第 2 のメディアの ID を所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録方法。

【請求項 5】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第 1 のメディアの ID に関する情報を ID 鍵として暗号化した第 1 の暗号化鍵情報とが記録された前記第 1 のメディアから、前記暗号化コンテンツ情報を第 2 のメディアに記録する際に、

前記第 1 のメディア側から前記暗号化コンテンツ情報と前記第 1 の暗号化鍵情報とを前記第 2 のメディア側に出し、

前記第 2 のメディア側で、前記暗号化コンテンツ情報を前記第 2 のメディアに記録すると共に、前記第 1 のメディア側から得た前記第 1 のメディアの ID に関する情報により一旦前記第 1 の暗号化鍵情報の暗号を解き、前記第 2 のメディアの ID に関する情報を ID 鍵として前記コンテンツ鍵を再暗号化した第 2 の暗号化鍵情報を前記第 2 のメディアに記録することを特徴とするコンテンツ情報記録方法。

【請求項 6】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第 1 のメディアの ID に関する情報を ID 鍵として暗号化した第 1 の暗号化鍵情報とが記録された前記第 1 のメディアから、前記暗号化コンテンツ情報を第 2 のメディアに記録する際に、

前記第 1 のメディア側で、一旦前記第 1 の暗号化鍵情報の暗号を解き、前記第 2 のメディア側から得た前記第 2 のメディアの ID に関する情報を ID 鍵として前記コンテンツ鍵を再暗号化して第 2 の暗号化鍵情報を得、その第 2 の暗号化鍵情報を前記第 2 のメディア側に出し、前記第 2 のメディア側で、前記第 1 のメディア側から出力された前記暗号化コンテンツ情報と前記第 2 の暗号化鍵情報とを前記第 2 のメディアに記録することを特徴とするコンテンツ情報記録方法。

【請求項 7】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第 1 のメディアの ID に関する情報を ID 鍵として暗号化した第 1 の暗号化鍵情報とが記録された前記第 1 のメディアから、前記暗号化コンテンツ情報を第 2 のメディアに記録する際に、下記方法 [a] と方法 [b] とを選択することを特

微とするコンテンツ情報記録方法。

方法〔a〕

前記第1のメディア側から前記暗号化コンテンツ情報と前記第1の暗号化鍵情報とを前記第2のメディア側に出
力し、

前記第2のメディア側で、前記暗号化コンテンツ情報を前記第2のメディアに記録すると共に、前記第1のメ
ディア側から得た前記第1のメディアのIDに関する情報により一旦前記第1の暗号化鍵情報の暗号を解き、前記
第2のメディアのIDに関する情報をID鍵として前記
コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記
第2のメディアに記録する。

方法〔b〕

前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から得た前記第2
のメディアのIDに関する情報をID鍵として前記コン
テンツ鍵を再暗号化して第2の暗号化鍵情報を得、その
第2の暗号化鍵情報を前記第2のメディア側に出力し、
前記第2のメディア側で、前記第1のメディア側から出
力された前記暗号化コンテンツ情報と前記第2の暗号化
鍵情報とを前記第2のメディアに記録する。

【請求項8】請求項5～7のいずれか一つに記載のコン
テンツ情報記録方法において、

前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であ
り、

前記第1の暗号化鍵情報のID鍵は、前記第1のメデ
ィアのIDをそのまま用いた共通鍵または前記第1のメデ
ィアのIDを所定の関数により変換した情報を用いた共
通鍵であり、

前記第2の暗号化鍵情報のID鍵は、前記第2のメデ
ィアのIDをそのまま用いた共通鍵または前記第2のメデ
ィアのIDを所定の関数により変換した情報を用いた共
通鍵であることを特徴とするコンテンツ情報記録方法。

【請求項9】第1のメディアのIDに関する情報をID
鍵としてコンテンツ情報を暗号化した第1の暗号化コン
テンツ情報が記録された前記第1のメディアから、前記
コンテンツ情報を第2のメディアに記録するコンテンツ
情報記録装置であって、

前記第2のメディア側において、前記第1のメディア側
から出力された前記第1のメディアのIDに関する情報
により、前記第1のメディア側から出力された前記第1
の暗号化コンテンツ情報の暗号を一旦解き、前記第2の
メディアのIDに関する情報をID鍵として前記コンテ
ンツ情報を再暗号化した第2の暗号化コンテンツ情報を
前記第2のメディアに記録させる記録手段を設けたこと
特徴とするコンテンツ情報記録装置。

【請求項10】第1のメディアのIDに関する情報をID
鍵としてコンテンツ情報を暗号化した第1の暗号化コン
テンツ情報が記録された前記第1のメディアから、前
記コンテンツ情報を第2のメディアに記録するコンテン

ツ情報記録装置であって、

前記第1のメディア側において、一旦前記第1の暗号化
コンテンツ情報の暗号を解き、前記第2のメディア側か
ら出力された前記第2のメディアのIDに関する情報を
ID鍵として前記コンテンツ情報を再暗号化して第2の
暗号化コンテンツ情報を得、その第2の暗号化コンテ
ンツ情報を前記第2のメディア側に出力させ、前記第2の
暗号化コンテンツ情報を前記第2のメディアに記録させ
る記録手段を設けたことを特徴とするコンテンツ情報記
録装置。

10 【請求項11】第1のメディアのIDに関する情報をID
鍵としてコンテンツ情報を暗号化した第1の暗号化コン
テンツ情報が記録された前記第1のメディアから、前
記コンテンツ情報を第2のメディアに記録する際に、下
記記録動作〔a〕と記録動作〔b〕とを選択する選択手
段を設けたことを特徴とするコンテンツ情報記録装置。

記録動作〔a〕

前記第2のメディア側において、前記第1のメディア側
から出力された前記第1のメディアのIDに関する情報
により、前記第1のメディア側から出力された前記第1
の暗号化コンテンツ情報の暗号を一旦解き、前記第2の
メディアのIDに関する情報をID鍵として前記コンテ
ンツ情報を再暗号化した第2の暗号化コンテンツ情報を
前記第2のメディアに記録させる。

記録動作〔b〕

20 前記第1のメディア側において、一旦前記第1の暗号化
コンテンツ情報の暗号を解き、前記第2のメディア側か
ら出力された前記第2のメディアのIDに関する情報を
ID鍵として前記コンテンツ情報を再暗号化して第2の
暗号化コンテンツ情報を得、その第2の暗号化コンテ
ンツ情報を前記第2のメディア側に出力させ、前記第2の
暗号化コンテンツ情報を前記第2のメディアに記録させ
る。

【請求項12】請求項9～11のいずれか一つに記載の
コンテンツ情報記録装置において、

前記第1の暗号化コンテンツ情報のID鍵は、前記第1
のメディアのIDをそのまま用いた共通鍵または前記第
1のメディアのIDを所定の関数により変換した情報を用
いた共通鍵であり、

40 前記第2の暗号化コンテンツ情報のID鍵は、前記第2
のメディアのIDをそのまま用いた共通鍵または前記第
2のメディアのIDを所定の関数により変換した情報を用
いた共通鍵であることを特徴とするコンテンツ情報記
録装置。

【請求項13】所定のコンテンツ鍵で暗号化された暗号
化コンテンツ情報と、前記コンテンツ鍵を第1のメデ
ィアのIDに関する情報をID鍵として暗号化した第1の
暗号化鍵情報とが記録された前記第1のメディアから、
前記暗号化コンテンツ情報を第2のメディアに記録する
コンテンツ情報記録装置であって、

前記第2のメディア側で、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1の暗号化鍵情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録させる暗号化鍵情報記録手段を設けたことを特徴とするコンテンツ情報記録装置。

【請求項14】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、

前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出力させ、前記第2の暗号化鍵情報を前記第2のメディアに記録させる暗号化鍵情報記録手段を設けたことを特徴とするコンテンツ情報記録装置。

【請求項15】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録する際に、下記記録動作〔a〕と記録動作〔b〕とを選択する選択手段を設けたことを特徴とするコンテンツ情報記録装置。

記録動作〔a〕

前記第2のメディア側で、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1の暗号化鍵情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録させる。

記録動作〔b〕

前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出力させ、前記第2の暗号化鍵情報を前記第2のメディアに記録させる。

【請求項16】請求項13～15のいずれか一つに記載のコンテンツ情報記録装置において、

前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、

前記第1の暗号化鍵情報のID鍵は、前記第1のメディアのIDをそのまま用いた共通鍵または前記第1のメ

ディアのIDを所定の関数により変換した情報を用いた共通鍵であり、

前記第2の暗号化鍵情報のID鍵は、前記第2のメディアのIDをそのまま用いた共通鍵または前記第2のメディアのIDを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツ情報を記録再生するコンテンツ情報配信システムに関するものである。そして、この発明はコンテンツ情報（特にオーディオやビデオのデータ）を配信し、配信されたデータの不正な譲渡、複製を阻止しながら、ユーザーのメディア間でのデータの譲渡、複製を安全に行うことのできるコンテンツ情報配信システムにおけるコンテンツ情報記録方法及びコンテンツ情報記録装置を提供することを目的としている。

【0002】

【従来の技術】暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのデジタルデータを配信する有用な方法として、特開平10-269289号公報に記載のデジタルコンテンツ配布管理方法、デジタルコンテンツ再生方法及び装置がある。この発明においては、デジタルコンテンツの配布側では、デジタルコンテンツを暗号化及び圧縮して加工し、この加工したデジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、デジタルコンテンツの再生側では、その加工されたデジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツに使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。また、特開平9-25303号公報に記載の情報記録媒体、記録装置、情報伝送システム、暗号解読装置がある。この発明の情報記録媒体は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるものにおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザー側で暗号化された情報をそのままHDDや光ディスクにコピーし、不正使用をすることを防止した。

【0003】

【発明が解決しようとする課題】しかしながら上記の従来の方式では、一度メディアに記録されたコンテンツデータを、ユーザー間で譲渡、複製することができない（メディア自体の譲渡はできてもそのメディアに記録さ

れたコンテンツデータの正規の再生ができない。)の
で、ユーザーがコンテンツデータを手に入れるために
は、一度は必ず課金管理機関、データ管理センター等に
接続しなければならない。また、1人のユーザーが複数
のメディアを持っていた場合、そのメディア間でデータ
を移動させることができない。暗号化を解いてコンテン
ツデータを伝送した場合にはコンテンツデータの譲渡、
複製は可能となるが、当然不正な譲渡、複製を許すこと
となりデータ伝送のセキュリティを確保できない。本発
明は、コンテンツ情報を配信し、配信されたデータの不正
な譲渡、複製を阻止しながら、ユーザーのメディア間
でのデータの譲渡、複製を安全に行うことのできるコン
テンツ情報配信システムにおけるコンテンツ情報記録方
法及びコンテンツ情報記録装置を提供することを目的と
している。

【0004】

【課題を解決するための手段】そこで、上記課題を解決
するために本発明は、下記の方法、装置を提供するもの
である。

(1) 第1のメディアのIDに関する情報をID鍵とし
てコンテンツ情報を暗号化した第1の暗号化コンテン
ツ情報が記録された前記第1のメディアから、前記コンテ
ンツ情報を第2のメディアに記録する際に、前記第1の
メディア側から前記第1の暗号化コンテンツ情報を前記
第2のメディア側に出し、前記第2のメディア側で、
前記第1のメディア側から得た前記第1のメディアのID
に関する情報により一旦前記第1の暗号化コンテン
ツ情報の暗号を解き、前記第2のメディアのIDに関する
情報をID鍵として前記コンテンツ情報を再暗号化した
第2の暗号化コンテンツ情報を前記第2のメディアに記
録することを特徴とするコンテンツ情報記録方法。

(2) 第1のメディアのIDに関する情報をID鍵とし
てコンテンツ情報を暗号化した第1の暗号化コンテン
ツ情報が記録された前記第1のメディアから、前記コンテ
ンツ情報を第2のメディアに記録する際に、前記第1の
メディア側で、一旦前記第1の暗号化コンテンツ情報の
暗号を解き、前記第2のメディア側から得た前記第2の
メディアのIDに関する情報をID鍵として前記コンテ
ンツ情報を再暗号化して第2の暗号化コンテンツ情報を
得、その第2の暗号化コンテンツ情報を前記第2のメデ
ィア側に出し、前記第2のメディア側で、前記第2の
暗号化コンテンツ情報を前記第2のメディアに記録する
ことを特徴とするコンテンツ情報記録方法。

(3) 第1のメディアのIDに関する情報をID鍵とし
てコンテンツ情報を暗号化した第1の暗号化コンテン
ツ情報が記録された前記第1のメディアから、前記コンテ
ンツ情報を第2のメディアに記録する際に、下記方法
[a]と方法[b]とを選択することを特徴とするコン
テンツ情報記録方法。

方法[a]

前記第1のメディア側から前記第1の暗号化コンテン
ツ情報を前記第2のメディア側に出し、前記第2のメデ
ィア側で、前記第1のメディア側から得た前記第1のメ
ディアのIDに関する情報により一旦前記第1の暗号化
コンテンツ情報の暗号を解き、前記第2のメディアのID
に関する情報をID鍵として前記コンテンツ情報を再
暗号化した第2の暗号化コンテンツ情報を前記第2のメ
ディアに記録する。

方法[b]

10 前記第1のメディア側で、一旦前記第1の暗号化コンテ
ンツ情報の暗号を解き、前記第2のメディア側から得た
前記第2のメディアのIDに関する情報をID鍵として
前記コンテンツ情報を再暗号化して第2の暗号化コンテ
ンツ情報を得、その第2の暗号化コンテンツ情報を前記
第2のメディア側に出し、前記第2のメディア側で、
前記第2の暗号化コンテンツ情報を前記第2のメディア
に記録する。

(4) 上記(1)～(3)のいずれか一つに記載のコン
テンツ情報記録方法において、前記第1の暗号化コンテ
ンツ情報のID鍵は、前記第1のメディアのIDをその
まま用いた共通鍵または前記第1のメディアのIDを所
定の関数により変換した情報を用いた共通鍵であり、前
記第2の暗号化コンテンツ情報のID鍵は、前記第2の
メディアのIDをそのまま用いた共通鍵または前記第2
のメディアのIDを所定の関数により変換した情報を用
いた共通鍵であることを特徴とするコンテンツ情報記録
方法。

(5) 所定のコンテンツ鍵で暗号化された暗号化コンテ
ンツ情報と、前記コンテンツ鍵を第1のメディアのID
に関する情報をID鍵として暗号化した第1の暗号化鍵
情報が記録された前記第1のメディアから、前記暗号
化コンテンツ情報を第2のメディアに記録する際に、前
記第1のメディア側から前記暗号化コンテンツ情報と前
記第1の暗号化鍵情報とを前記第2のメディア側に出し、
前記第2のメディア側で、前記暗号化コンテンツ情報
を前記第2のメディアに記録すると共に、前記第1の
メディア側から得た前記第1のメディアのIDに関する
情報により一旦前記第1の暗号化鍵情報の暗号を解き、
前記第2のメディアのIDに関する情報をID鍵として
前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を
前記第2のメディアに記録することを特徴とするコンテ
ンツ情報記録方法。

(6) 所定のコンテンツ鍵で暗号化された暗号化コンテ
ンツ情報と、前記コンテンツ鍵を第1のメディアのID
に関する情報をID鍵として暗号化した第1の暗号化鍵
情報が記録された前記第1のメディアから、前記暗号
化コンテンツ情報を第2のメディアに記録する際に、前
記第1のメディア側で、一旦前記第1の暗号化鍵情報の
暗号を解き、前記第2のメディア側から得た前記第2の
メディアのIDに関する情報をID鍵として前記コンテ

ンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出し、前記第2のメディア側で、前記第1のメディア側から出力された前記暗号化コンテンツ情報と前記第2の暗号化鍵情報とを前記第2のメディアに記録することを特徴とするコンテンツ情報記録方法。

(7) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録する際に、下記方法[a]と方法[b]とを選択することを特徴とするコンテンツ情報記録方法。

方法[a]

前記第1のメディア側から前記暗号化コンテンツ情報と前記第1の暗号化鍵情報とを前記第2のメディア側に出し、前記第2のメディア側で、前記暗号化コンテンツ情報を前記第2のメディアに記録すると共に、前記第1のメディア側から得た前記第1のメディアのIDに関する情報により一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録する。

方法[b]

前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から得た前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出し、前記第2のメディア側で、前記第1のメディア側から出力された前記暗号化コンテンツ情報と前記第2の暗号化鍵情報とを前記第2のメディアに記録する。

(8) 上記(5)～(7)のいずれか一つに記載のコンテンツ情報記録方法において、前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、前記第1の暗号化鍵情報のID鍵は、前記第1のメディアのIDをそのまま用いた共通鍵または前記第1のメディアのIDを所定の関数により変換した情報を用いた共通鍵であり、前記第2の暗号化鍵情報のID鍵は、前記第2のメディアのIDをそのまま用いた共通鍵または前記第2のメディアのIDを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録方法。

(9) 第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、前記第2のメディア側において、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1のメディア側から出力された前記第1の暗号化コンテンツ情報の暗号を一旦

解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化した第2の暗号化コンテンツ情報を前記第2のメディアに記録させる記録手段を設けたこと特徴とするコンテンツ情報記録装置。

(10) 第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、前記第1のメディア側において、一旦前記第1の暗号化コンテンツ情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化して第2の暗号化コンテンツ情報を得、その第2の暗号化コンテンツ情報を前記第2のメディア側に出し、前記第2の暗号化コンテンツ情報を前記第2のメディアに記録させる記録手段を設けたこと特徴とするコンテンツ情報記録装置。

(11) 第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録する際に、下記記録動作[a]と記録動作[b]とを選択する選択手段を設けたこと特徴とするコンテンツ情報記録装置。

記録動作[a]

前記第2のメディア側において、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1のメディア側から出力された前記第1の暗号化コンテンツ情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化した第2の暗号化コンテンツ情報を前記第2のメディアに記録させる。

記録動作[b]

前記第1のメディア側において、一旦前記第1の暗号化コンテンツ情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化して第2の暗号化コンテンツ情報を得、その第2の暗号化コンテンツ情報を前記第2のメディア側に出し、前記第2の暗号化コンテンツ情報を前記第2のメディアに記録させる。

(12) 上記(9)～(11)のいずれか一つに記載のコンテンツ情報記録装置において、前記第1の暗号化コンテンツ情報のID鍵は、前記第1のメディアのIDをそのまま用いた共通鍵または前記第1のメディアのIDを所定の関数により変換した情報を用いた共通鍵であり、前記第2の暗号化コンテンツ情報のID鍵は、前記第2のメディアのIDをそのまま用いた共通鍵または前記第2のメディアのIDを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録装置。

(13) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、前記第2のメディア側で、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1の暗号化鍵情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録させる暗号化鍵情報記録手段を設けたことを特徴とするコンテンツ情報記録装置。

(14) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出力させ、前記第2の暗号化鍵情報を前記第2のメディアに記録させる暗号化鍵情報記録手段を設けたことを特徴とするコンテンツ情報記録装置。

(15) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録する際に、下記記録動作[a]と記録動作[b]とを選択する選択手段を設けたことを特徴とするコンテンツ情報記録装置。
記録動作[a] 前記第2のメディア側で、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1の暗号化鍵情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録させる。

記録動作[b]

前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出力させ、前記第2の暗号化鍵情報を前記第2のメディアに記録させる。

(16) 上記(13)～(15)のいずれか一つに記載のコンテンツ情報記録装置において、前記所定のコンテ

ンツ鍵は共通鍵もしくは公開鍵であり、前記第1の暗号化鍵情報のID鍵は、前記第1のメディアのIDをそのまま用いた共通鍵または前記第1のメディアのIDを所定の関数により変換した情報を用いた共通鍵であり、前記第2の暗号化鍵情報のID鍵は、前記第2のメディアのIDをそのまま用いた共通鍵または前記第2のメディアのIDを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録装置。

【0005】

10 【発明の実施の形態】本発明によれば、不正な譲渡、複製を防止しつつ、メディアに記録されたコンテンツデータをユーザー間で譲渡、複製することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。また、本発明によれば、1人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの譲渡、複製を行えるシステムを提供できる。さらに、常に暗号化されたセキュリティの高い状態でコンテンツデータを譲渡、複製することができる。

20 【0006】本発明では、

(1) 第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録する際に、前記第1のメディア側から前記第1の暗号化コンテンツ情報を前記第2のメディア側に出力し、前記第2のメディア側で、前記第1のメディア側から得た前記第1のメディアのIDに関する情報により一旦前記第1の暗号化コンテンツ情報の暗号を解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化した第2の暗号化コンテンツ情報を前記第2のメディアに記録するようにした。

(2) 第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録する際に、前記第1のメディア側で、一旦前記第1の暗号化コンテンツ情報の暗号を解き、前記第2のメディア側から得た前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化して第2の暗号化コンテンツ情報を得、その第2の暗号化コンテンツ情報を前記第2のメディア側に出力し、前記第2のメディア側で、前記第2の暗号化コンテンツ情報を前記第2のメディアに記録するようにした。

(3) 第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録する際に、下記方法[a]と方法[b]とを選択するようにした。

50 方法[a]

前記第1のメディア側から前記第1の暗号化コンテンツ情報を前記第2のメディア側に出し、前記第2のメディア側で、前記第1のメディア側から得た前記第1のメディアのIDに関する情報により一旦前記第1の暗号化コンテンツ情報の暗号を解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化した第2の暗号化コンテンツ情報を前記第2のメディアに記録する。

方法〔b〕

前記第1のメディア側で、一旦前記第1の暗号化コンテンツ情報の暗号を解き、前記第2のメディア側から得た前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化して第2の暗号化コンテンツ情報を得、その第2の暗号化コンテンツ情報を前記第2のメディア側に出し、前記第2のメディア側で、前記第2の暗号化コンテンツ情報を前記第2のメディアに記録する。

（4）上記（1）～（3）のいずれか一つに記載のコンテンツ情報記録方法において、前記第1の暗号化コンテンツ情報のID鍵は、前記第1のメディアのIDをそのまま用いた共通鍵または前記第1のメディアのIDを所定の関数により変換した情報を用いた共通鍵であり、前記第2の暗号化コンテンツ情報のID鍵は、前記第2のメディアのIDをそのまま用いた共通鍵または前記第2のメディアのIDを所定の関数により変換した情報を用いた共通鍵であるようにした。

（5）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録する際に、前記第1のメディア側から前記暗号化コンテンツ情報と前記第1の暗号化鍵情報とを前記第2のメディア側に出し、前記第2のメディア側で、前記暗号化コンテンツ情報を前記第2のメディアに記録すると共に、前記第1のメディア側から得た前記第1のメディアのIDに関する情報により一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録するようにした。

（6）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録する際に、前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から得た前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出し、前

記第2のメディア側で、前記第1のメディア側から出力された前記暗号化コンテンツ情報と前記第2の暗号化鍵情報とを前記第2のメディアに記録するようにした。

（7）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録する際に、下記方法〔a〕と方法〔b〕とを選択するようにした。

10 方法〔a〕

前記第1のメディア側から前記暗号化コンテンツ情報と前記第1の暗号化鍵情報とを前記第2のメディア側に出し、前記第2のメディア側で、前記暗号化コンテンツ情報を前記第2のメディアに記録すると共に、前記第1のメディア側から得た前記第1のメディアのIDに関する情報により一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録する。

20 方法〔b〕

前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から得た前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出し、前記第2のメディア側で、前記第1のメディア側から出力された前記暗号化コンテンツ情報と前記第2の暗号化鍵情報とを前記第2のメディアに記録する。

30 （8）上記（5）～（7）のいずれか一つに記載のコンテンツ情報記録方法において、前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、前記第1の暗号化鍵情報のID鍵は、前記第1のメディアのIDをそのまま用いた共通鍵または前記第1のメディアのIDを所定の関数により変換した情報を用いた共通鍵であり、前記第2の暗号化鍵情報のID鍵は、前記第2のメディアのIDをそのまま用いた共通鍵または前記第2のメディアのIDを所定の関数により変換した情報を用いた共通鍵であるようにした。

40 （9）第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、前記第2のメディア側において、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1のメディア側から出力された前記第1の暗号化コンテンツ情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化した第2の暗号化コンテンツ情報を前記第2のメディアに記録させる記録
50 手段を設けるようにした。

(10) 第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、前記第1のメディア側において、一旦前記第1の暗号化コンテンツ情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化して第2の暗号化コンテンツ情報を得、その第2の暗号化コンテンツ情報を前記第2のメディア側に出力させ、前記第2の暗号化コンテンツ情報を前記第2のメディアに記録させる記録手段を設けるようにした。

(11) 第1のメディアのIDに関する情報をID鍵としてコンテンツ情報を暗号化した第1の暗号化コンテンツ情報が記録された前記第1のメディアから、前記コンテンツ情報を第2のメディアに記録する際に、下記記録動作[a]と記録動作[b]とを選択する選択手段を設けるようにしたコンテンツ情報記録装置。

記録動作[a]

前記第2のメディア側において、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1のメディア側から出力された前記第1の暗号化コンテンツ情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化した第2の暗号化コンテンツ情報を前記第2のメディアに記録させる。

記録動作[b]

前記第1のメディア側において、一旦前記第1の暗号化コンテンツ情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ情報を再暗号化して第2の暗号化コンテンツ情報を得、その第2の暗号化コンテンツ情報を前記第2のメディア側に出力させ、前記第2の暗号化コンテンツ情報を前記第2のメディアに記録させる。

(12) 上記(9)～(11)のいずれか一つに記載のコンテンツ情報記録装置において、前記第1の暗号化コンテンツ情報のID鍵は、前記第1のメディアのIDをそのまま用いた共通鍵または前記第1のメディアのIDを所定の関数により変換した情報を用いた共通鍵であり、前記第2の暗号化コンテンツ情報のID鍵は、前記第2のメディアのIDをそのまま用いた共通鍵または前記第2のメディアのIDを所定の関数により変換した情報を用いた共通鍵であるようにした。

(13) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、前記第2のメディア側で、

前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1の暗号化鍵情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録させる暗号化鍵情報記録手段を設けるようにした。

(14) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録するコンテンツ情報記録装置であって、前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出力させ、前記第2の暗号化鍵情報を前記第2のメディアに記録させる暗号化鍵情報記録手段を設けるようにした。

(15) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第1のメディアのIDに関する情報をID鍵として暗号化した第1の暗号化鍵情報とが記録された前記第1のメディアから、前記暗号化コンテンツ情報を第2のメディアに記録する際に、下記記録動作[a]と記録動作[b]とを選択する選択手段を設けるようにしたコンテンツ情報記録装置。

記録動作[a]

前記第2のメディア側で、前記第1のメディア側から出力された前記第1のメディアのIDに関する情報により、前記第1の暗号化鍵情報の暗号を一旦解き、前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化した第2の暗号化鍵情報を前記第2のメディアに記録させる。

記録動作[b]

前記第1のメディア側で、一旦前記第1の暗号化鍵情報の暗号を解き、前記第2のメディア側から出力された前記第2のメディアのIDに関する情報をID鍵として前記コンテンツ鍵を再暗号化して第2の暗号化鍵情報を得、その第2の暗号化鍵情報を前記第2のメディア側に出力させ、前記第2の暗号化鍵情報を前記第2のメディアに記録させる。

(16) 上記(13)～(15)のいずれか一つに記載のコンテンツ情報記録装置において、前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、前記第1の暗号化鍵情報のID鍵は、前記第1のメディアのIDをそのまま用いた共通鍵または前記第1のメディアのIDを所定の関数により変換した情報を用いた共通鍵であり、前記第2の暗号化鍵情報のID鍵は、前記第2のメディアのIDをそのまま用いた共通鍵または前記第2のメディアのIDを所定の関数により変換した情報を用いた共通

鍵であるようにした。

【0007】まず、図2を用いて本発明の一実施例の構成を説明する。メディアはメディア固有のIDが設定され、メディア制御器にセットすることが出来る。メディアは記録再生可能であり、固有のIDを設定可能なものであれば、固体メモリーやディスク、テープ等でも良い。但し、ID情報が所定の耐タンパー性をもつことが条件である。即ち、IDや暗号化に必要な鍵の保管に対して不正に情報を読み出したり、書き換えたりするのが難しい状態になっていることが望ましい。

【0008】もっとも簡単なものはメモリータイプでこのメモリーカードは所定のメモリー制御器を介してしか、IDや暗号化鍵情報が引き出せない仕組みになっているものが、安全で簡単に作成できる。メモリーカードは、工場生産時にカード毎に固有なIDが記録されている。もしくは発行装置により発行される際に、そのメモリー固有のIDをEEPROMなどに記録された後、樹脂封入等で埋めこまれるようになっている。これにより、後からユーザ対応鍵情報が変更できない、つまり不正改ざんできないようにする。メディアには一部のデータのみメディア間のコピーを行うことの出来るメディアバスを有している。

【0009】メディア制御器はメディアをセットして、PCもしくは専用器などの端末に接続し、メディア内のデータと、端末とのインターフェース機能と、所定のIDでのデータの暗号化、復号化機能を有する。メディア制御器は端末側からメモリーの内部を不正にアクセスできない耐タンパー性をもっている。端末は外部にあるコンテンツ情報を配信をするセンター（配信センター）に接続し、課金、認証など所定の手続きを経て、コンテンツデータを受信する。センターとの接続はインターネットなどのネットワークはもちろん、ISDNや放送、ケーブルTV、PHSなどの無線接続でもかまわない。

【0010】コンテンツ情報は基本的にコンテンツ毎に違う鍵（コンテンツ鍵）で暗号化される。コンテンツはMPEGなどの所定の圧縮方式によって圧縮された後、DESなどの暗号化がなされている。例えばDESの場合、暗号化鍵は64ビット程度である。データベースとセンターと端末の関係を図1に示す。センターに設置したデータベースで、コンテンツ情報が、コンテンツX1を暗号化鍵G1で暗号化し、また、違うコンテンツX2を暗号化鍵G2で暗号化するものとして管理されている。

【0011】このセンターには複数の端末がネットワークで接続されている。端末への送信もセキュリティーを考慮して公開鍵方式で暗号化して送信する。ここで端末1（T1）の公開鍵をT1Pとし、復号鍵をT1Dとすると、データベース1に管理されていたコンテンツX1は、暗号化鍵G1で暗号化されEG1(X1)という暗号化コンテンツ情報とされる。暗号化鍵G1は、端末T1に送信するために端末T1の公開鍵T1Pを使用して暗号化され、暗号化鍵の情報ET

1P(G1)となる。そして、暗号化コンテンツ情報EG1(X1)と暗号化鍵の情報ET1P(G1)との2つの情報を端末1（T1）に送信する。

【0012】端末1でこのコンテンツ情報を再生するためには、端末1の復号鍵T1Dを用いて、暗号化鍵の情報ET1P(G1)を復号し、暗号化鍵G1を得て、その暗号化鍵G1で暗号化コンテンツ情報EG1(X1)を復号し、コンテンツX1を得て、MPEGなどの復号を行うことで再生することが出来るが、ここでは、送信されたデータを端末で再生することなく、すぐに端末に接続されたメディアに記録することを前提とする。ここでは公開鍵を使って端末までのデータ送信を説明したが、これは、共通鍵方式であっても、また他の方式であっても本発明はサポートすることが出来る。

【0013】次に図3、4、5を用いて本発明のコンテンツ情報と鍵情報の受け渡し機能について説明する。最初に配信センターから端末T1側のメディアA（第1のメディア）にコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器にセットする。
20 メディア制御器を端末T1にセットして、「データ記録モード」にする。課金、認証など所定の手続きを行う。手続きが終了すると、センターからコンテンツデータが所定の暗号化鍵G1で暗号化されて端末に配信されてくる。

【0014】即ち、コンテンツXを暗号化鍵G1で暗号化した暗号化コンテンツ情報EG1(X)が送信されてくる。また、暗号化鍵G1を端末T1に送信するために、端末T1の公開鍵T1Pを使用して暗号化鍵G1を暗号化した暗号化鍵情報ET1P(G1)が端末T1に送信されてくる。端末で復号
30 に使用する鍵はT1Dなので、この暗号化鍵情報ET1P(G1)は復号鍵T1Dで復号できる。この状態をET1D(G1)と表現する。端末ではこの暗号化鍵情報ET1D(G1)を一度復号鍵T1Dで復号して暗号化鍵G1を得る。復号した暗号化鍵G1でコンテンツデータXを復号し、このコンテンツデータXをメディアAに転送する。

【0015】メディアにおいてコンテンツをメディアのIDによって暗号化し直す方式について図3を用いて説明する。メディア制御器はこのコンテンツデータXを受信したら、メディア制御器内部でメディアAのIDをID鍵として暗号化し直す。メディアAには第1の暗号化
40 コンテンツ情報EA(X)が記録される。この暗号化コンテンツデータをそのまま、メディアBにコピーしてもメディアBではID=Bであるので、このEA(X)を再生することは出来ない。しかしながら、メディアAで復号して、再生できる状態の生信号データをメディアBへ転送するのはセキュリティ上問題がある。

【0016】そこで、図3（1）のようにメディアA側でコピー先メディアのID=Bを読み取り、先にメディアA側でID=AをID鍵として暗号化されたコンテンツデータを復号し、コピー先のID=BをID鍵として
50

再暗号化して第2の暗号化コンテンツ情報EB(X)としてメディアBに転送する。

【0017】もしくは、図3(2)のようにID=Aで暗号化されたコンテンツデータEA(X)を、そのままメディアBへ転送し、メディアB側で、コピー元のメディアAのIDを読み取り、ID=Aで暗号化されたコンテンツデータを復号し、ID=Bで再暗号化してEB(X)として記録する。これにより、コンテンツデータはどちらかのIDで暗号化されている状態で転送されるのでセキュリティが確保される。なお、一つの記録装置において、図3(1)に示す方法と図3(2)に示す方法とのどちらか一方を任意に選択できるようにしてもよい。

【0018】次に、コンテンツ鍵(暗号化鍵)で暗号化された暗号化コンテンツ情報と、これに使用したコンテンツ鍵(暗号化鍵)をさらにそのメディアもしくは端末のIDに関する情報をID鍵として暗号化している場合について図4を用いて説明する。最初に配信センターから端末T1側のメディアA(第1のメディア)にコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器にセットする。メディア制御器を端末T1にセットして、「データ記録モード」にする。課金、認証など所定の手続きを行う。手続きが終了すると、センターからコンテンツデータが所定の暗号化鍵G1で暗号化されて端末に配信されてくる。

【0019】即ち、コンテンツXを暗号化鍵G1で暗号化した暗号化コンテンツ情報EG1(X)が送信されてくる。また、暗号化鍵G1を端末T1に送信するために、端末T1の公開鍵T1Pを使用して暗号化鍵G1を暗号化した暗号化鍵情報ET1P(G1)が端末T1に送信されてくる。端末で復号に使用する鍵はT1Dなので、この暗号化鍵情報ET1P(G1)は復号鍵T1Dで復号できる。この状態をET1D(G1)と表現する。端末ではこの暗号化鍵情報ET1D(G1)を一度復号鍵T1Dで復号して暗号化鍵G1を得る。

【0020】メディア制御器ではこのデータを受信し、メディアAには暗号化コンテンツ情報EG1(X)が記録され、同時にメディア制御器はセットされたメディアのIDを認識して、この鍵G1をメディアAの固有のIDであるAという値で再暗号化して第1の暗号化鍵情報EA(G1)得、これをメディアAに記録する。このときのデータ構造例を図5に示す。暗号化コンテンツ情報のヘッダーに64ビットの暗号化鍵情報が記録される。この構造は必ずしも、一体化している必要はなく、対になっていることが管理できれば分離されていてもかまわない。

【0021】この第1の暗号化鍵情報EA(G1)をそのままメディアBにコピーしても、メディアBではID=Bであるので、このEA(G1)を復号することは出来ない。そこで、図4(1)のようにメディアA側でコピー先メディアのID=Bを読み取り、先にメディアA側でID=Aで暗号化された第1の暗号化鍵情報EA(G1)を復号

し、コピー先のID=Bで再暗号化して第2の暗号化鍵情報EB(G1)にしてメディアBに転送する。もしくは図4(2)のようにID=Aで暗号化された第1の暗号化鍵情報EA(G1)を、そのままメディアBへ転送し、メディアB側で、コピー元のメディアAのIDを読み取り、ID=Aで暗号化された第1の暗号化鍵情報EA(G1)を復号し、ID=Bで再暗号化して第2の暗号化鍵情報EB(G1)にして記録する。

【0022】このように、コンテンツデータが暗号化されている状態EG1(X)で転送されるばかりでなく、暗号化鍵G1もどちらかのメディアのIDで暗号化されている状態(EA(G1)またはEB(G1))で転送されるのでセキュリティが確保される。コンテンツデータXの容量が大きい場合、図4に示すように、暗号化コンテンツ情報EG1(X)の暗号化鍵(コンテンツ鍵)G1をさらにそのメディアもしくは端末のIDに関する情報をID鍵として暗号化する方式(EA(G1)またはEB(G1)を用いる方式)を用いたほうが、鍵情報だけを復号化、暗号化するだけでコピーできるので、高速にハンドリングが可能である。なお、一つの記録装置において、図4(1)に示す方法と図4(2)に示す方法とのどちらか一方を任意に選択できるようにしてもよい。

【0023】次に、図6を用いて本発明のコンテンツ情報記録装置の一実施例のブロック図について説明する。このブロック図は暗号化鍵(コンテンツ鍵)G1をさらにそのメディアもしくは端末のIDに関する情報をID鍵として暗号化する方式(EA(G1)またはEB(G1)を用いる方式)によるものであり、図4(1)のメディアAからメディアBへの記録を例に説明する。

【0024】最初に配信センターからメディアAにコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器21にセットする。メディア制御器21を端末T1にセットして、外部インターフェースよりメディア制御器21のモード設定部51に「データ記録モード」を設定する。課金、認証など所定の手続きが終了すると、センターからコンテンツデータXが所定の暗号化鍵G1で暗号化されて暗号化コンテンツ情報EG1(X)として端末T1に配信されてくる。「データ記録モード」の場合、モード設定部51はスイッチ1とスイッチ2を鍵暗号化部52に接続するように切り替える。

【0025】センターからは、暗号化コンテンツ情報EG1(X)と共に、暗号化鍵G1を端末T1に送信するためにT1の公開鍵T1Pを使用して暗号化鍵G1を暗号化したET1P(G1)が送信されてくる。端末T1で復号に使用する鍵はT1Dなのでこの暗号化鍵情報ET1P(G1)はT1Dで復号できる。この状態をET1D(G1)と表現する。端末T1ではこの暗号化鍵情報ET1D(G1)を一度T1Dで復号する。

【0026】メディア制御器21ではこのデータを受信し、メディアAにはこのEG1(X)が記録され、メディアB

御器 21 はセットされたメディア A の ID をメディア ID 読み取り部 53 で認識して、鍵暗号化部 52 で暗号化鍵 G1 を ID=A で暗号化し、暗号化鍵情報 EA(G1) を暗号化鍵情報書き込み部 54 に送信する。暗号化鍵情報書き込み部 54 では、暗号化鍵情報を、メディア A に記録されている暗号化コンテンツ情報 EG1(X) のヘッダー 64 ビットに記録する。

【0027】次に、メディア A に記録されている暗号化コンテンツ情報 EG1(X) を再生する場合を説明する。メディア A をメディア制御器 21 にセットし、外部インターフェースよりメディア制御器 21 のモード設定部 51 に「データ再生モード」を設定する。メディア A 側のメディア ID 発生部 31 により発生された信号は、メディア制御器 21 のメディア ID 読み取り部 53 によってメディアの ID=A を検出し、暗号化復号部 56 に送信する。

【0028】メディア制御部 21 はメディア A のメモリー部 32 から暗号化コンテンツ情報 EG1(X) を読み出し、暗号化鍵情報読み取り部 55 に送信する。暗号化鍵情報読み取り部 55 は、先頭にある暗号化鍵情報 64 ビットを読み、スイッチ 1 を介して暗号化鍵情報 EA(G1) を暗号化鍵復号部 56 へ送信する。モード設定部 51 によって「データ再生モード」の場合、スイッチ 1 は暗号化鍵復号部 56 側へ切り替えられている。

【0029】暗号化鍵復号部 56 では、入力されたメディア ID=A を使用して、暗号化鍵情報 EA(G1) を復号する。復号した暗号化鍵 G1 は暗号化コンテンツデータ復号部 57 に送信される。また、暗号化鍵情報読み取り部 55 でヘッダーが取り去られた暗号化コンテンツデータは暗号化コンテンツデータ復号部 57 に送信される。暗号化コンテンツデータ復号部 57 では、入力された暗号化コンテンツデータ EG1(X) と暗号化鍵 G1 によって暗号化コンテンツデータを復号化し、再生データとして出力する。

【0030】次に、メディア A からメディア B へコンテンツデータをコピーする場合を説明する。コンテンツの記録されているコピー元メディア A からコピー先メディア B に暗号化コンテンツ情報 EG1(X) をコピーする場合、まず、メディア制御器 21 にメディア A をセットする。外部インターフェースよりメディア制御器 21 のモード設定部 51 に「データコピー出力モード」を設定する。

【0031】メディア A のメディア ID 発生部 31 により発生された信号は、メディア制御器 21 のメディア ID 読み取り部 53 によってメディアの ID=A が検出し、暗号化鍵復号部 56 に送信される。モード設定部 51 に「データコピー出力モード」と設定されているとき、スイッチ 1、2 は、暗号化鍵復号部 56 につながるように切り替えられている。

【0032】メディア A に記録されていた暗号化コンテンツ情報 EG1(X) は暗号化鍵情報読み取り部 55 に送信され、ここでヘッダー 64 ビットの暗号化鍵情報 EA

(G1) が読み取られる。読み取られた暗号化鍵情報 EA(G1) は暗号化鍵復号部 56 に送信される。暗号化鍵復号部 56 では、入力された ID=A と暗号化鍵情報 EA(G1) から暗号化鍵 G1 を復号し、鍵メモリー 58 に一時記録する。

【0033】一方、暗号化コンテンツデータ EG1(X) は、メディア A 側のメモリー部 32 のデータ移動用領域に格納され、メディアバス 33 を介して、メディアバス 33 に接続されるメディア B に高速に転送される。このメディアバスは、メディア A とメディア B を物理的に連結してデータ転送する。転送するデータ自体は暗号化コンテンツデータのみがこのメディアバスを通過できるようになっているので安全性が高い。

【0034】次に、メディア制御器 21 にメディア B をセットする。メディア制御器 21 のメディア ID 読み取り部 53 によってメディアの ID=B を検出する。モード設定部 51 に「データコピー入力モード」と設定されているとき、スイッチ 1、2 は鍵暗号化部 52 につながるように切り替えられている。鍵暗号化部 52 では、鍵メモリー 58 から暗号化鍵 G1 を読み出し、メディア ID 読み取り部 53 から入力された ID=B を使用して、暗号化鍵 G1 を ID=B で暗号化し EB(G1) とする。暗号化鍵情報 EB(G1) は暗号化鍵情報書き込み部 54 に送信される。暗号化鍵情報 EB(G1) はメディア B のメモリー部 32 B に記録される。

【0035】メディア B に記録された暗号化コンテンツ情報 EG1(X) を再生する場合を説明する。これはメディア A に記録された暗号化コンテンツ情報 EG1(X) を再生する場合と同じである。即ち、メディア B をメディア制御器 21 にセットし、外部インターフェースよりメディア制御器 21 のモード設定部 51 に「データ再生モード」を設定する。メディア B 側のメディア ID 発生部 31 B により発生された信号は、メディア制御器 21 のメディア ID 読み取り部 53 によってメディアの ID=B を検出し、暗号化復号部 56 に送信する。

【0036】メディア制御部 21 はメディア B のメモリー部 32 B から暗号化コンテンツ情報 EG1(X) を読み出し、暗号化鍵情報読み取り部 55 に送信する。暗号化鍵情報読み取り部 55 は、先頭にある暗号化鍵情報 64 ビットを読み、スイッチ 1 を介して暗号化鍵情報 EB(G1) を暗号化鍵復号部 56 へ送信する。モード設定部 51 によって「データ再生モード」の場合、スイッチ 1 は暗号化鍵復号部 56 側へ切り替えられている。

【0037】暗号化鍵復号部 56 では、入力されたメディア ID=B を使用して、暗号化鍵情報 EB(G1) を復号する。復号した暗号化鍵 G1 は暗号化コンテンツデータ復号部 57 に送信される。また、暗号化鍵情報読み取り部 55 でヘッダーが取り去られた暗号化コンテンツデータは暗号化コンテンツデータ復号部 57 に送信される。暗号化コンテンツデータ復号部 57 では、入力された暗号

化コンテンツデータ $E_{G1}(X)$ と暗号化鍵 $G1$ によって暗号化コンテンツデータを復号化し、再生データとしてコンテンツデータ X を出力する。

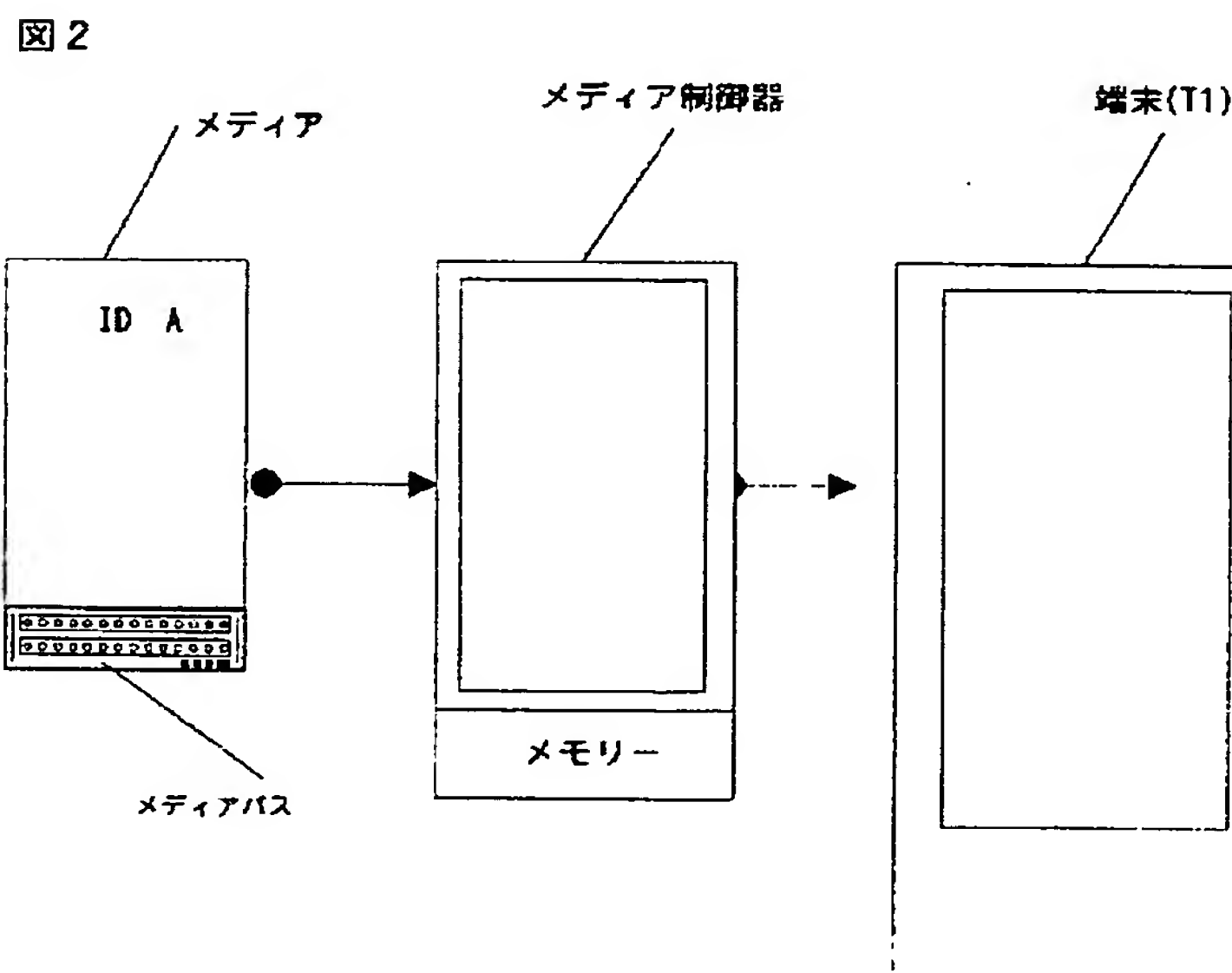
【0038】このように、本実施例の記録装置では、コンテンツデータが暗号化されている状態 $E_{G1}(X)$ で転送されるばかりでなく、暗号化鍵 $G1$ もメディア B の ID で暗号化されている状態 ($E_B(G1)$) で転送されるのでセキュリティが確保される。上記実施例では、暗号化鍵 $G1$ を復号化しメディア B の ID で再暗号化する処理を送信側 (メディア A 側) で行った。よって、受信専用のメディア制御器には鍵暗号化部 52、スイッチ 1、2 は不要となり、システムとして限定されたユーザーのみ送信できるというシステムを構築することが可能となる。

【0039】なお、メディア A からメディア B へコンテンツデータをコピー (複製) ではなく譲渡する場合には、メディア A 側から暗号化鍵情報 $E_A(G1)$ 及び暗号化コンテンツデータ $E_{G1}(X)$ の内の少なくとも一方を消去する。

【0040】また、図3 (1) に示す方法と実現する記録装置としては、メディア A 側において、一旦第1の暗号化コンテンツ情報 $E_A(X)$ の暗号を解き、メディア B 側から出力されたメディア B の $ID=B$ を ID 鍵としてコンテンツ情報を再暗号化して第2の暗号化コンテンツ情報 $E_B(X)$ を得、その第2の暗号化コンテンツ情報 $E_B(X)$ をメディア B 側に出力させ、第2の暗号化コンテンツ情報 $E_B(X)$ をメディア B に記録させる記録手段を設ける。

【0041】

【図2】



【発明の効果】以上の通り、本発明によれば、不正な譲渡、複製を防止しつつ、メディアに記録されたコンテンツデータをユーザー間で譲渡、複製することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。また、この発明によれば、1人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの譲渡、複製を行えるシステムを提供できる。さらには、常に暗号化されたセキュリティの高い状態でコンテンツデータを譲渡、複製することができる。

【図面の簡単な説明】

【図1】一実施例に用いるデータ配信時の暗号化を説明するための図である。

【図2】一実施例の構成例を示す図である。

【図3】一実施例の機能説明図である。

【図4】一実施例の他の機能説明図である。

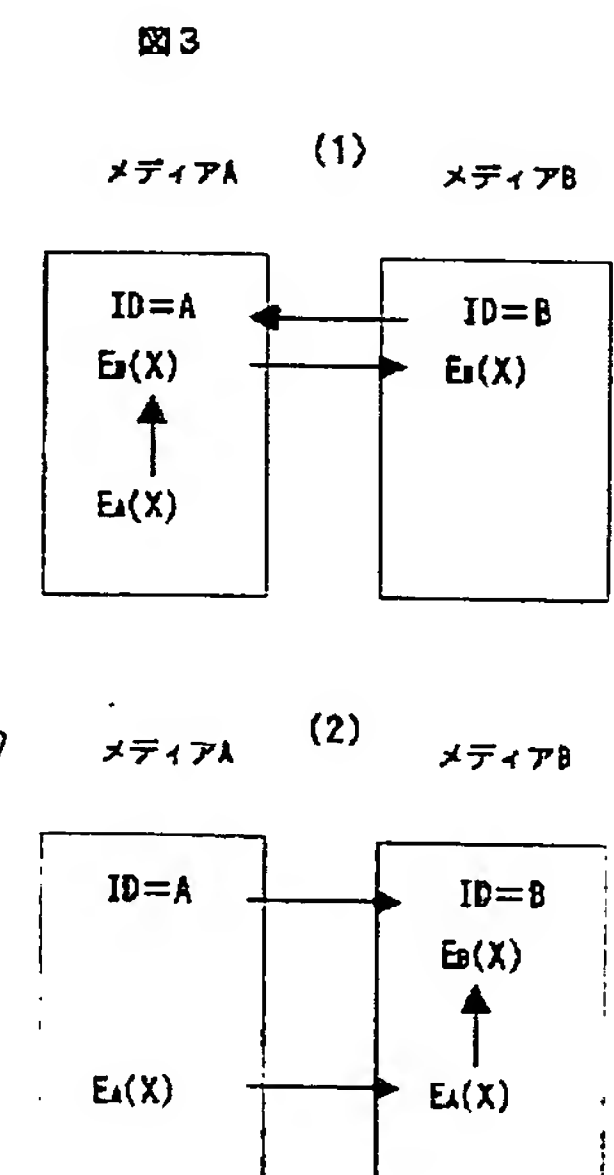
【図5】一実施例のメディア内のデータ構造図である。

【図6】一実施例の詳細構成を示すブロック図である。

【符号の説明】

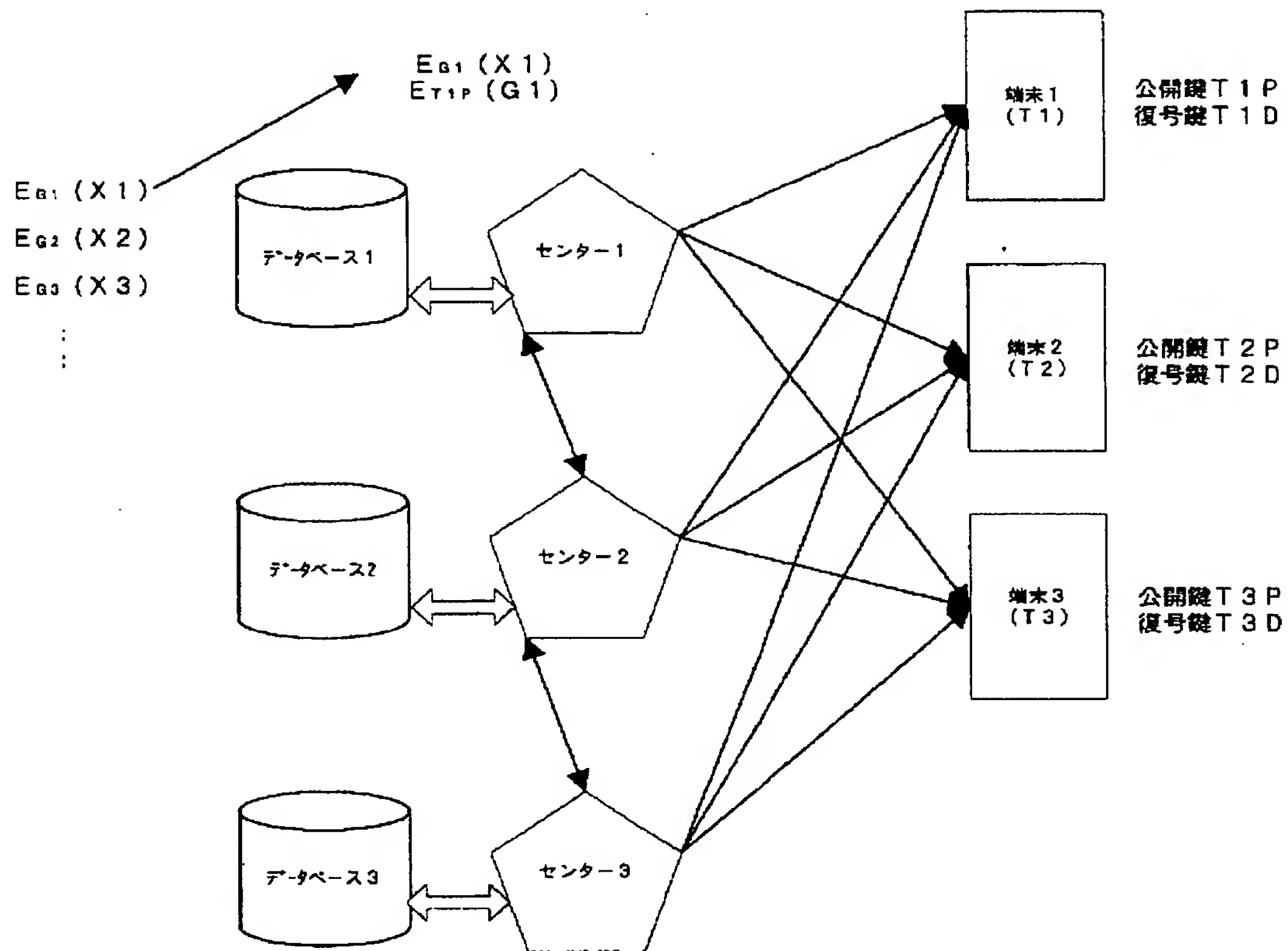
- 20 21 メディア制御器
51 モード設定部
52 鍵暗号化部
53 メディアID読み取り部
54 暗号化鍵情報書き込み部
55 暗号化鍵情報読み取り部
56 暗号化鍵復号部
57 暗号化コンテンツデータ復号部
58 鍵メモリー

【図3】



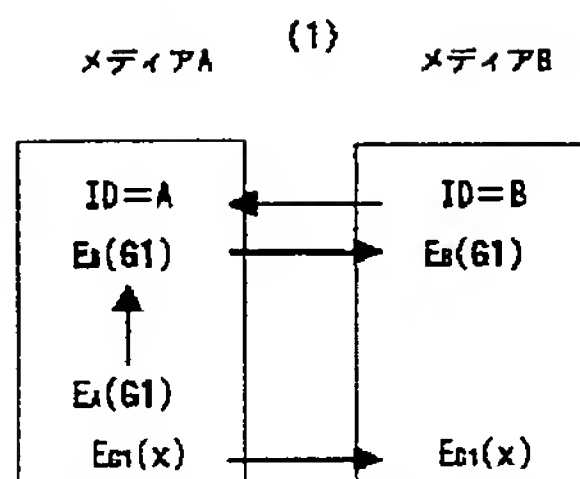
【図1】

図1



【図4】

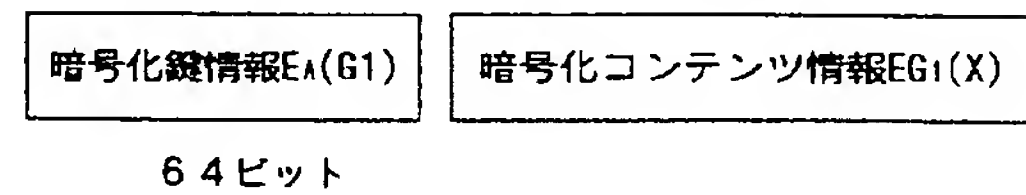
図4



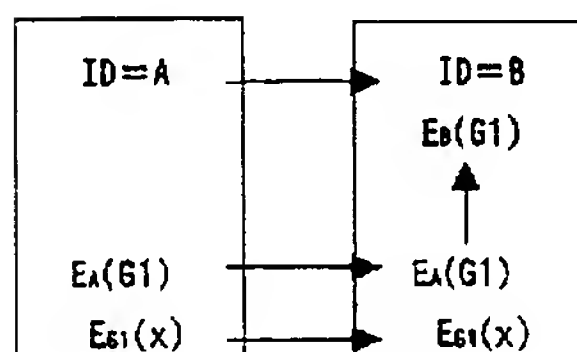
【図5】

図5

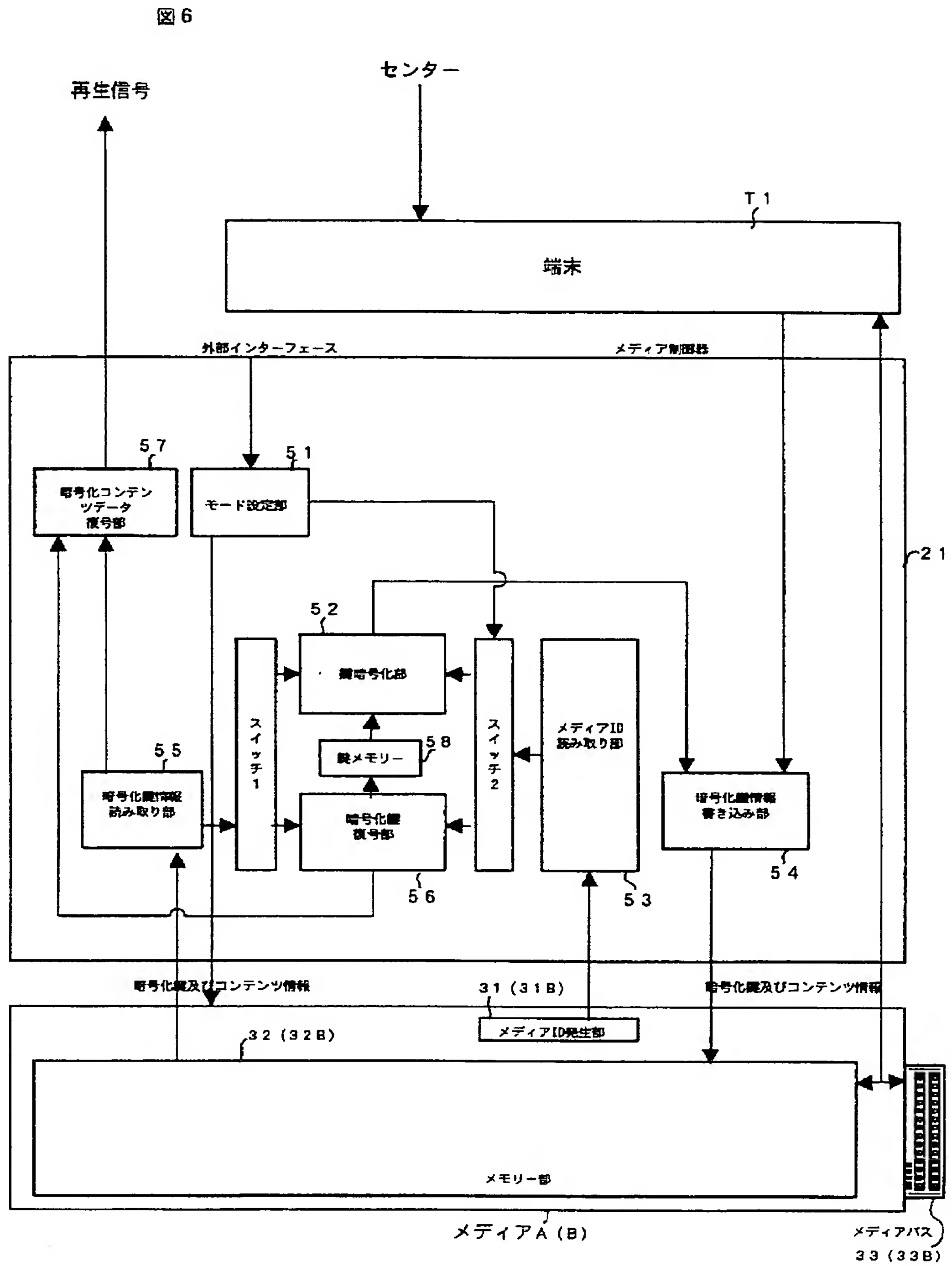
メディア内データ構造



メディアA (2) メディアB



【図6】



THIS PAGE BLANK (USPTO)